(19) Japan Patent Office (JP)

(12) Laid-open Patent Gazette (A)

(11) Laid-open patent application number
Tokkai H. 11-259571

(43) Date of laying-open: Sept. 24, 1999

(51) Int. Cl.[6]	Identification number	FI
G06F		G06F 340Z
17/60		15/21 C
11/34		11/34 330
		15/21

Request for examination: not filed; number of claims: 25; OL (10 pp in all)

(21) Application number: Patent application H. 10-63013

(22) Application date: March 13, 1998

(71) Applicant: 000004226
NTT Inc.,
19-2 Nishishinjuku 3-chome, Shinjuku-ku, Tokyo

(72) Inventor: Hitoshi Fuji
c/o NTT Inc., 19-2 Nishishinjuku 3-chome, Shinjuku-ku, Tokyo

(72) Inventor: Takeji Nakayama
c/o NTT Inc., 19-2 Nishishinjuku 3-chome, Shinjuku-ku, Tokyo

(72) Inventor: Masashi Ijuin
c/o NTT Inc., 19-2 Nishishinjuku 3-chome, Shinjuku-ku, Tokyo

(74) Agent: patent attorney Takehiko Suge

(54) [Title of the invention] Method of detecting unauthorized use of electronic commerce transaction system and device therefor

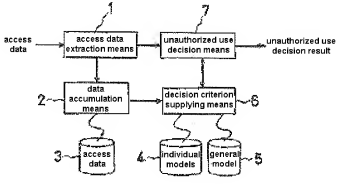
(57) [Abstract]

[Problem] To provide a method of detecting unauthorized use of an electronic commerce transaction system and a device therefor, capable of detecting unauthorized use of a system by an unauthorized user and/or an unauthorized client, based on the results of

monitoring the ordinary actions of regular users and/or regular clients.

[Means for solution] There are provided: decision criterion supplying means 6 that supplies a plurality of data items incorporated in individual models and a general model accumulated by data accumulation means 2 as a decision criterion for deciding whether or not the access in question is unauthorized access every time new access is executed; and unauthorized use decision means 7 that decides whether or not the access in question is based on unauthorized use, by comparing a plurality of data items incorporated in individual models and a general model provided by this decision criterion supplying means 6 with a plurality of new data items extracted by access data extraction means 1 accompanying the access in question.

α: device for detecting unauthorized use of electronic commerce transaction system



[Claims]

[Claim 1] A method for detecting unauthorized use of an electronic commerce transaction system wherein, in detection in real time by constant monitoring for unauthorized use of electronic commerce transactions on each access,

decision and detection are performed by referring to past action history trends and behavior in actions such as access or events by regular users and/or regular clients.

[Claim 2] The method for detecting unauthorized use

of an electronic commerce transaction system as claimed in claim 1, wherein said action history is divided into individual models and a general model.

[Claim 3] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 1 or 2, wherein said individual models and general model are mutually given orders of reference priority.

[Claim 4] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 2 or 3, wherein said individual models and general model make use of both data directly obtained from an individual record of events accompanying access; and

data derived from a plurality of event records.

[Claim 5] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 1, 2, 3 or 4, wherein, as said past action history, users and/or clients are given individual identifiers, and the function of these users and/or clients is controlled by means of data that is sent to said users and/or clients from this provider and/or server, such that, when a shift to a page subsequent to the initial screen takes place, this information is automatically transmitted to the provider and/or server and data sorted to each said individual identifier is accumulated in for example a file or memory in this provider or server.

[Claim 6] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 2, 3, 4 or 5, wherein said individual models and general model include both data on which statistical processing is performed and data expressing state transitions.

[Claim 7] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 6, wherein said state transitions include individual access action state transitions whereby unauthorized use is detected from access actions; and

plural access state transitions whereby unauthorized use is detected by comparison of state transitions from the past to the present.

[Claim 8] A method for detecting unauthorized use of an electronic commerce transaction system wherein, in detecting unauthorized use of electronic commerce transactions for detecting unauthorized use of an arbitrary client/server system whereby electronic commerce transactions are performed,

every time a prescribed event is issued a plurality of times from a client after commencement of access from said client to the server, said server sequentially acquires, as a plurality of data items, information relating to said client and the user, and also information relating to the electronic commerce transaction conduct of this user, and incorporates and accumulates this plurality of respective data items in an individual model identified as a unit by the individual identifier given to said user; and

thereafter, every time a new access is implemented, compares the plurality of data items obtained after commencement of this access with said individual model and decides whether or not this access is unauthorized use in accordance with the result of this comparison.

[Claim 9] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 8, wherein, in accumulation of said plurality of data items, said plurality of respective data items are incorporated in a general model for obtaining average user data of all the users using this system, instead of in said individual model; and

the decision as to whether or not said access is unauthorized use is made in accordance with the results of comparison of said plurality of data items and this general model.

[Claim 10] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 8 or 9, wherein accumulation of said plurality of data items is performed in accordance with

time sequence data whereby all of the data obtained at the time point where a single access has been terminated are arranged in order of their generation.

[Claim 11] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 10, wherein, when obtaining said time sequence data, the events up to this prescribed last event at a time-point where a prescribed limiting time has elapsed after the time at which said prescribed events are presumed to have been finally issued are regarded as a series of prescribed events included in a single access.

[Claim 12] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 8, 9, 10 or 11, wherein the decision as to whether or not said access is unauthorized use is made using a statistical technique.

[Claim 13] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 8, 9, 10, 11 or 12, wherein the decision as to whether or not said access is unauthorized use is made by detecting irregularity of state transition of this system accompanying said prescribed event issued a plurality of times during a single access.

[Claim 14] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 8, 9, 10, 11 or 12, wherein the decision as to whether or not said access is unauthorized use is made by detecting irregularity of specified data, of said plurality of data items presumed to be of the same user acquired in a plurality of accesses.

[Claim 15] The method for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 14, wherein said specified data is data comprising information relating to said electronic commerce transactions by said user.

[Claim 16] The method for detecting unauthorized

use of an electronic commerce transaction system as claimed in claim 8, 9, 10, 11, 12, 13, 14 or 15, wherein said prescribed event is a next-screen display request event for requesting display of the next screen.

[Claim 17] A device for detecting unauthorized use of an electronic commerce transaction system equipped with: access data extraction means that extracts at least access data sent from a client to an arbitrary server in a client/server system whereby electronic commerce transactions are performed with commencement of access, and data accumulation means that accumulates said access data extracted by this access data extraction means; wherein

said access data extraction means, in addition to extraction of said access data, is given the function of extracting a plurality of data items including information relating to said client and the user and information relating to the electronic commerce transaction conduct of this user, every time a prescribed event is issued a plurality of times from said client after commencement of said access; and

said data accumulation means, in addition to accumulation of said access data, is given the function of incorporating and accumulating said plurality of respective data items extracted by said access data extraction means in an individual model identified as a unit by the individual identifier given to said user;

and which comprises:

decision criterion supplying means that supplies a plurality of data items incorporated in said individual model accumulated by this data accumulation means as a decision criterion for deciding whether or not this access is unauthorized use every time new access is executed; and

unauthorized use decision means that decides whether or not this access is unauthorized use by comparing a plurality of data items incorporated in said individual model supplied by this decision

criterion supplying means with the new plurality of data items extracted by said access data extraction means accompanying this access.

[Claim 18] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17, wherein it is given the series of respective organically linked functions and

said data accumulation means incorporates said respective plurality of data in a general model for obtaining average data of all of the users using this system instead of in said individual model,

said decision criterion supplying means supplies as the decision criterion for deciding whether or not this access is unauthorized use, a plurality of data items incorporated in said general model accumulated by this data accumulation means, every time new access is executed, and

said unauthorized use decision means decides whether or not this access is unauthorized use by comparing a plurality of data items incorporated in said general model supplied by this decision criterion supplying means with the new plurality of data items extracted by said access data extraction means accompanying this access.

[Claim 19] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17 or 18, wherein

said data accumulation means has a function of performing accumulation of said plurality of data items in accordance with time sequence data whereby all of the data items obtained at the time point where a single access has terminated are arranged in order of their generation.

[Claim 20] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 18, wherein said data accumulation means, when obtaining said time sequence data, has a function of regarding the events up to this prescribed last event at a time-point where a prescribed limiting

time has elapsed after the time at which said prescribed events are presumed to have been finally issued as a series of prescribed events included in a single access.

[Claim 21] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17, 18, 19 or 20, wherein said unauthorized use decision means comprises calculation means that effects the decision as to whether or not said access is unauthorized use using a statistical technique.

[Claim 22] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17, 18, 19, 20 or 21, wherein said unauthorized use decision means comprises calculation means that effects the decision as to whether or not said access is unauthorized use by detecting irregularity of state transition of this system accompanying said prescribed event issued a plurality of times during a single access.

[Claim 23] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17, 18, 19, 20 or 21, wherein said unauthorized use decision means comprises calculation means that effects the decision as to whether or not said access is unauthorized use by detecting irregularity of specified data items of said plurality of data items presumed to be those of the same user acquired in a plurality of accesses.

[Claim 24] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 23, wherein said specified data items are data comprising information relating to said electronic commerce transaction performed by said user.

[Claim 25] The device for detecting unauthorized use of an electronic commerce transaction system as claimed in claim 17, 18, 19, 20, 21, 22, 23 or 24, wherein said prescribed event is a next-screen display request event for requesting display of the next

screen.

[Detailed description of the invention]

[0001]

[Technical field to which the invention belongs]

The present invention relates to a method and device for detecting unauthorized use of an electronic commerce transaction system. In more detail, it relates to a method for detecting unauthorized use of an electronic commerce transaction system for detecting unauthorized use of this electronic transaction system whereby a person who has not been granted permission to use an arbitrary client/server system (hereinbelow simply referred to as an "electronic commerce transaction system") for performing the sale of products etc by using electronic commerce transactions poses as a person who has properly been granted permission, and to a device for detecting unauthorized use of the electronic commerce transaction system that is directly employed to put this into practice.

[0002]

[Prior art] In recent years, virtual malls, i.e. electronic shopping arcades, have been constructed whereby the sale of products can be performed by for example displaying product catalogues on a WWW site on the Internet using for example the WWW (World Wide Web).

[0003] With a WWW site of this type, a user (user who is attempting to purchase a product) inputs the user's own credit card information from a client terminal or performs electronic commerce transactions by effecting settlement using electronic money, so, in the event of unauthorized use, the operator of the shopping arcade may suffer monetary damage. In order to prevent this, a server must detect unauthorized use during the short time from commencement of access of the electronic commerce transaction system by the user to settlement thereof and exclude the unauthorized user.

[0004] What is meant by "unauthorized use" in this

context is that another person acquires by some method other than the regular procedure an individual identifier such as an ID (identification) or password that was acquired from the server administrator through the regular procedure by a given person, and proceeds to utilize the server functions by using this, or that the server functions are utilized by impersonating another person using a defect of the system. Hereinbelow, the expression "unauthorized user" means a person who performs such unauthorized use.

[0005] Examples of methods of detection of unauthorized use adopted in typical conventional computer systems are as follows:

(1) a technique in which, by analyzing the various logs that are kept in the computer system, for example execution of a command which is not allowed to the user is detected, and this is deemed to be unauthorized use.

[0006] (2) a technique in which the system administrator, for example, investigates beforehand events that might be the subject of attack from a person trying to perform unauthorized use by examining for example defects of the software used to constitute the computer system, mis-settings, or inappropriate use thereof.

[0007] (3) a technique of, by means of a system that is permanently resident in the computer system, or a system that performs monitoring of network packets, arranged on the network, monitoring the actions (history of event requests) of privileged users (this indicates users having system administration rights i.e. so-called superusers, distinguished from ordinary users) capable of damaging the computer system and comparing these with the pattern of action registered beforehand in the system, and thereby deciding whether such actions are those of an unauthorized user.

[0008]

[Problem that the invention is intended to solve] However, the techniques for detection of unauthorized use indicated above are merely techniques that are

already adopted in typical computer systems. In the case of technique (1), the required detection of unauthorized use can only be performed with the timing with which the logs are periodically inspected, so no benefit can be expected in the case of an electronic commerce transaction system, in which detection of unauthorized use in real time is demanded.

[0009] In the case of technique (2), it is only possible to check for defects whose existence is recognized beforehand, so unauthorized use that is performed in a situation in which no defects or the like are present cannot be detected: thus, for the same reasons as described above, application of this technique to electronic commerce transaction systems is difficult.

[0010] Also, in the case of technique (3), this only functions in conditions in which there are privileged user actions that can be the subject of monitoring and so basically cannot be employed to monitor for unauthorized users from among users having the same privileges. In particular, in the case of the electronic commerce transaction systems in question, no privileged user is present in the registered users and all the users have the same privileges so what they can do in the server is the same.

[0011] As described above, none of these techniques can be applied to detection of unauthorized use of an electronic commerce transaction system. That is, from the above, for detection of unauthorized use of an electronic commerce transaction system, rather than monitoring the actions of privileged users, it appears more appropriate to perform this detection on the basis of the ordinary actions of regular users and for this purpose, the best strategy is of course the use of the logs recorded in the server as the electronic commerce transaction system is accessed.

[0012] However, when considering the types of log that are recorded in a server as described above, a WWW server for example records in logs only extremely

restricted information, specifically, the filename in respect of which a request for display is made from a client, the machine name of the client that is the source of the request, or the time etc.

[0013] Furthermore, a characteristic feature of a WWW server is that sessions comprising display requests from the same client can only be recorded in discrete fashion for each occasion. This means that display requests for a plurality of pages performed with same object by a user cannot be captured as a series of actions performed by the same user.

[0014] Accordingly, the chief objects to be solved by the present invention are as follows. Specifically, a first object of the present invention is to provide a method and device for detection of unauthorized use of an electronic commerce transaction system capable of detecting unauthorized use of the system by an unauthorized user, based on the results of monitoring the ordinary actions of regular users.

[0015] A second object of the present invention is to provide a method and device for detection of unauthorized use of an electronic commerce transaction system whereby it is possible to grasp a series of actions performed by the same user.

[0016] A third object of the present invention is to provide a method and device for detection of unauthorized use of an electronic commerce transaction system capable of detecting unauthorized use of the system based on the style of actions of typical users.

[0017] Other objects on the present invention will become clear from the description of the specification, drawings and in particular the claims.

[0018]

[Means for solving the problem] The present invention is characterized by the provision of a technique and means whereby, for solving the above problems, a plurality of data items of various types issued after commencement of access of the server by a client are acquired, the respective plurality of data

items, once these have been acquired, are compared with a plurality of data items obtained after this access every time new access is executed, and a decision is made as to whether or not this access is unauthorized use in accordance with the result of this comparison.

[0019] To describe the invention in further detail, in the solution of these problems, the above objects are achieved according to the present invention by the adoption of novel characteristic constituent techniques and means, extending from the above general concept to subordinate concepts and listed by way of example as follows.

[0020] Specifically, according to a first characteristic feature of the method according to the present invention, in detection in real time by constant monitoring for unauthorized use of electronic commerce transactions on each access, a method is adopted of detection of unauthorized use of the electronic commerce transaction system by decision and detection performed referring to past action history trends and behavior in actions such as access or events by regular users and/or regular clients.

[0021] According to a second characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein said action history in the first characteristic feature of the method according to the present invention is divided into individual models and a general model.

[0022] According to a third characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein said individual models and general model according to the first or second characteristic features of the method according to the present invention are mutually given orders of reference priority.

[0023] According to a fourth characteristic feature of the method according to the present invention, a

method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein said individual models and general model according to the second or third characteristic features of the method according to the present invention make use of both data directly obtained from an individual record of events accompanying access; and data derived from a plurality of event records.

[0024] According to a fifth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein, as said past action history according to the first, second, third or fourth characteristic features of the method according to the present invention, users and/or clients are given individual identifiers, and the function of these users and/or clients is controlled by means of data that is sent to said users and/or clients from this provider and/or server, such that, when a shift to a page subsequent to the initial screen takes place, this information is automatically transmitted to the provider and/or server and data sorted to each said individual identifier is accumulated in for example a file or memory in this provider or server.

[0025] According to a sixth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein said individual models and general model according to the first, second, third, fourth or fifth characteristic features of the method according to the present invention include both data on which statistical processing is performed and data expressing state transitions.

[0026] According to a seventh characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein said state transitions according to the

sixth characteristic feature of the method according to the present invention include individual access action state transitions whereby unauthorized use is detected from access actions; and plural access state transitions whereby unauthorized use is detected by comparison of state transitions from the past to the present.

[0027] According to an eighth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein, in detecting unauthorized use of electronic commerce transactions for detecting unauthorized use of an arbitrary client/server system whereby electronic commerce transactions are performed, every time a prescribed event is issued a plurality of times from a client after commencement of access from the client to the server, the server sequentially acquires, as a plurality of data items, information relating to the client and the user, and also information relating to the electronic commerce transaction conduct of this user, and incorporates and accumulates this plurality of respective data items in an individual model identified as a unit by the individual identifier given to the user; and thereafter, every time a new access is implemented, compares the plurality of data items obtained after commencement of this access with the individual model and decides whether or not this access is unauthorized use in accordance with the result of this comparison.

[0028] According to a ninth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein, in accumulation of the plurality of data items according to the eighth characteristic feature of the method according to the present invention, the plurality of respective data items are incorporated in a general model for obtaining average user data of all the users

using this system, instead of in the individual model; and the decision as to whether or not the access is unauthorized use is made in accordance with the results of comparison of the plurality of data items and this general model.

[0029] According to a tenth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein accumulation of the plurality of data items according to the eigth or ninth characteristic feature of the method according to the present invention is performed in accordance with time sequence data whereby all of the data obtained at the time point where a single access has been terminated are arranged in order of their generation.

[0030] According to an eleventh characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein, when obtaining the time sequence data according to the tenth characteristic feature of the method according to the present invention, the events up to this prescribed last event at a time-point where a prescribed limiting time has elapsed after the time at which the prescribed events are presumed to have been finally issued are regarded as a series of prescribed events included in a single access.

[0031] According to a twelfth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein the decision as to whether or not the access according to the eighth, ninth, tenth or eleventh characteristic features of the method according to the present invention is unauthorized use is made using a statistical technique.

[0032] According to a thirteenth characteristic feature of the method according to the present

invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein the decision as to whether or not the access according to the eighth, ninth, tenth, eleventh or twelfth characteristic features of the method according to the present invention is unauthorized use is made by detecting irregularity of state transition of this system accompanying the prescribed event issued a plurality of times during a single access.

[0033] According to a fourteenth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein the decision as to whether or not the access according to the eighth, ninth, tenth, eleventh or twelfth characteristic features of the method according to the present invention is unauthorized use is made by detecting irregularity of specified data, of the plurality of data items presumed to be of the same user acquired in a plurality of accesses.

[0034] According to a fifteenth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein the specified data according to the fourteenth characteristic feature of the method according to the present invention is data comprising information relating to the electronic commerce transactions by the user.

[0035] According to a sixteenth characteristic feature of the method according to the present invention, a method is adopted of detection of unauthorized use of the electronic commerce transaction system wherein the prescribed event according to the eighth, ninth, tenth, eleventh, twelfth, thirteenth, fourteenth or fifteenth characteristic features of the method according to the present invention is a next-screen display request event for requesting display of the next screen.

[0036] According to a first characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system equipped with: access data extraction means that extracts at least access data sent from a client to an arbitrary server in a client/server system whereby electronic commerce transactions are performed with commencement of access, and data accumulation means that accumulates access data extracted by this access data extraction means; wherein the access data extraction means, in addition to extraction of the access data, is given the function of extracting a plurality of data items including information relating to the client and the user and information relating to the electronic commerce transaction conduct of this user, every time a prescribed event is issued a plurality of times from the client after commencement of access; and the data accumulation means, in addition to accumulation of access data, is given the function of incorporating and accumulating the plurality of respective data items extracted by the access data extraction means in an individual model identified as a unit by the individual identifier given to the user; and comprising: decision criterion supplying means that supplies a plurality of data items incorporated in the individual model accumulated by this data accumulation means as a decision criterion for deciding whether or not this access is unauthorized use every time new access is executed; and unauthorized use decision means that decides whether or not this access is unauthorized use by comparing a plurality of data items incorporated in the individual model supplied by this decision criterion supplying means with the new plurality of data items extracted by the access data extraction means accompanying this access.

[0037] According to a second characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of

an electronic commerce transaction system that is given the series of respective organically linked functions wherein the data accumulation means in the first characteristic feature of the device according to the present invention incorporates the respective plurality of data in a general model for obtaining average data of all of the users using this system instead of in the individual model, the decision criterion supplying means supplies, as the decision criterion for deciding whether or not this access is unauthorized use, a plurality of data items incorporated in the general model accumulated by this data accumulation means, every time new access is executed, and the unauthorized use decision means decides whether or not this access is unauthorized use by comparing a plurality of data items incorporated in the general model supplied by this decision criterion supplying means with the new plurality of data items extracted by the access data extraction means accompanying this access.

[0038] According to a third characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the data accumulation means in the first or second characteristic feature of the device according to the present invention has a function of performing accumulation of the plurality of data items in accordance with time sequence data whereby all of the data items obtained at the time point where a single access has terminated are arranged in order of their generation.

[0039] According to a fourth characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the data accumulation means in the third characteristic feature of the device according to the present invention, when obtaining the time sequence data, has a function of regarding the events up to this prescribed

last event at a time-point where a prescribed limiting time has elapsed after the time at which the prescribed events are presumed to have been finally issued as a series of prescribed events included in a single access.

[0040] According to a fifth characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the unauthorized use decision means in the first, second, third or fourth characteristic feature of the device according to the present invention comprises calculation means that effects the decision as to whether or not the access is unauthorized use using a statistical technique.

[0041] According to a sixth characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the unauthorized use decision means in the first, second, third, fourth or fifth characteristic feature of the device according to the present invention comprises calculation means that effects the decision as to whether or not said access is unauthorized use by detecting irregularity of state transition of this system accompanying the prescribed event issued a plurality of times during a single access.

[0042] According to a seventh characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the unauthorized use decision means in the first, second, third, fourth or fifth characteristic feature of the device according to the present invention comprises calculation means that effects the decision as to whether or not said access is unauthorized use by detecting irregularity of specified data items of the plurality of data items presumed to be those of the same user acquired in a

plurality of accesses.

[0043] According to an eighth characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the specified data items in the seventh characteristic feature of the device according to the present invention are data comprising information relating to the electronic commerce transaction performed by the user.

[0044] According to a ninth characteristic feature of the device according to the present invention, a device is adopted for detection of unauthorized use of an electronic commerce transaction system wherein the prescribed event in the first, second, third, fourth, fifth, sixth, seventh or eighth characteristic feature of the device according to the present invention is a next-screen display request event for requesting display of the next screen.

[0045]

[Embodiments of the invention] Embodiments of the present invention are described below with reference to the appended drawings in terms of examples of the device and examples of the method thereof. It should be noted that, while, in the following description, in order to facilitate comprehension, an Internet system using the WWW is given as an example of a client/server system, the invention could likewise be applied to a user/provider system.

[0046] (Device example) Figure 1 is a block diagram showing the principles of the construction of a device for detection of unauthorized use of an electronic commerce transaction system according to an embodiment of the present invention.

[0047] As shown in this Figure, a device α for detection of unauthorized use of an electronic commerce transaction system according to this embodiment, as a precondition, is arranged on a server (not shown) in an arbitrary client/server system that performs electronic

commerce transactions, and comprises at least: access data extraction means 1 that extracts access data transmitted from a client (not shown) on commencement of access; and data accumulation means 2 that accumulates access data extracted by this access data extraction means 1. It should be noted that the access data that is accumulated by the data accumulation means 2 is in fact stored on access data storage means 3 comprising for example a hard disk.

[0048] In this device α for detection of unauthorized use of an electronic commerce transaction system, the aforesaid access data extraction means 1, in addition to extraction of the above access data, is given the function of extracting a plurality of data items including information relating to the client and information relating to the electronic commerce transaction conduct of this client, every time an event (next-screen display request event) for example for requesting display of the next screen is issued a plurality of times from the client after commencement of access.

[0049] At the same time, the data accumulation means 2, in addition to accumulation of access data in the access data storage means 3, is given the function of incorporating and accumulating the plurality of respective data items extracted by the access data extraction means 1 in an individual model identified as a unit by the individual identifier given to the client, and a general model for obtaining average data of all of the clients that utilize this system. It should be noted that the plurality of data items accumulated by the data accumulation means 2 are respectively stored in individual model storage means 4 comprising for example a hard disk and general model storage means 5, for the individual models and the general model.

[0050] In addition, this device α for detection of unauthorized use of an electronic commerce transaction system comprises: decision criterion supplying means 6

that supplies a plurality of data items incorporated in the individual model and general model by this data accumulation means 2 in individual model storage means 4 and general model storage means 5 as a decision criterion for deciding whether or not this access is unauthorized use every time new access is executed; and unauthorized use decision means 7 that decides whether or not this access is unauthorized use by comparing a plurality of data items incorporated in the individual model supplied by this decision criterion supplying means 6 with the new plurality of data items extracted by the access data extraction means 1 accompanying this access, using logical calculation means etc., not shown.

[0051] The accumulation of the plurality of data items by the data accumulation means 2 may be performed by means of time sequence data whereby all of the data obtained at the time-point where a single access terminated are arranged in order of generation thereof.

[0052] However, since for example in a WWW server, no means exists for ascertaining that access has been interrupted, the technique may be adopted of, when obtaining such time sequence data, at the time-point where a prescribed limiting time has elapsed from the time assumed to be that of the last issuance of an event, regarding the events up to the last event in question as a series of events included in a single access, in order to make the actions of the client continuous, for convenience (after lapse of the prescribed limiting time, these are not regarded as a series of events).

[0053] Also, while, in the unauthorized use decision means 7, the decision as to whether or not access represents unauthorized use is made using ordinary statistical techniques that make use of for example calculation means, further, as a special technique, irregularity of state transitions of the system of question accompanying events issued a plurality of times during a single access may be

detected, or, alternatively, of a plurality of data items assumed to be those of the same client acquired during a plurality of accesses, irregularity of specified data items comprising information relating to electronic commerce transactions performed by the client may be detected (details to be described later).

[0054] (Example of method) Next, an example of a method applied to an example of a device constructed as described above will be described in terms of its outline and implementation procedure.

[0055] [Outline] First of all, in order to capture the actions of a client accessing a WWW server in the server as a series of actions, the types of data that can be recorded by the WWW server are increased by installation of a CGI (Common Gateway Interface) or middleware.

[0056] Also, by giving the clients individual identifiers such as IDs, it is arranged to control client functions by means of data sent from the server to the clients such that, when a shift takes place to a page subsequent to the initial screen, information in respect of this is automatically transmitted to the server, and to accumulate the data apportioned to each individual identifier in for example a file or memory (access data storage means 3) in the server.

[0057] By means of this data, more information can be recorded than is recorded in the case of the standard WWW server logs, so that, even in a situation where a plurality of persons access the WWW server substantially at the same time point, the actions of specified individuals in the WWW server can be extracted.

[0058] In this connection, what is used for identifying regular clients and unauthorized clients is two types of data groups, namely, the individual models and general model described above. An individual model is a set of data that, for each individual identifier, saves an action history representing the trends and behavior of the client performed on the WWW server in

question in the past. The general model is a set of data expressing the trends and behavior found from all of the clients on this WWW server.

[0059] In either model, both data directly obtained from individual event recordings and data derived from a plurality of event recordings are utilized. The plurality of event recordings represent the result of aggregating the series of actions recorded for each individual identifier after commencement of access of the WWW server.

[0060] The individual model and general model herein include both data for the performance of statistical processing and data expressing state transitions. Data for the performance of statistical processing means data capable of being numerically quantified: the differences between the individual models or general model expressing the trends or behavior obtained by numerical quantification and persons having an individual identifier in the current access are verified using for example testing by a statistical technique. In addition, this data includes both data obtained from access to the WWW server on a single occasion only and data obtained from access to the WWW server on more than one occasion.

[0061] Also, in regard to state transition, two types of detection method are employed. One of these detection methods employs single access state transition, in which for example after the action of accessing the WWW server at a given time, an attempt to purchase a product without having perused the catalogue is detected and deemed to be unauthorized use. Another of these detection methods employs multiple access state transitions, in which an unauthorized client is detected by comparing past to present state transitions, in which for example a client, being a client whose total value of purchases has continued to rise over the past three purchasing occasions, attempts to make a purchase involving a sum larger than five times the average of the monetary amount of previous

purchases.

[0062] In either case, a rule constituting a criterion for regarding a client as an unauthorized client is registered beforehand and a client matching this rule is deemed to be an unauthorized client. However, these rules are modified by being cumulatively recalculated every time client access increases, so they should not have fixed values.

[0063] [Implementation procedure] First of all, when commencement of access of the WWW server by a client using an individual identifier is detected in the access data extraction means 1, the data accumulation means 2 commences recording of the access data relating to this individual identifier in the access recording means 3. At this time point, since, as the information of the connection source, the client's IP address (IP: Internet Protocol) and type of browser etc are obtained, these items of information are employed as a single item of information for identifying regular clients and unauthorized clients when detecting whether or not access is unauthorized use.

[0064] Next, by sequentially recording the actions relating to movement between pages subsequently performed in the server by the client, i.e. next-screen display request events, in the individual model storage means 4 and general model storage means 5 by using the access data extraction means 1 and data accumulation means 2, it is arranged to treat these as time sequence data from the instant where the client accessed the WWW server.

[0065] In the above state, when new access is detected by the access data extraction means 1 and an attempt is made to decide whether or not this access is unauthorized use, the decision criterion supplying means 6 reads the corresponding individual model and general model stored in the individual model storage means 4 and general model storage means 5 and supplies these as decision criteria to the unauthorized use

decision means 7.

[0066] This unauthorized use decision means 7 then, using (or selectively using) the individual model and general model that are supplied thereto, decides whether or not the access is unauthorized use by statistical processing and a comparison with the state transition rules, and transfers the result of this decision as to unauthorized use to the server processor (not shown). It should be noted that the criteria for detection of unauthorized use will not be fixed criteria, since they will depend on the object of the electronic commerce transaction system, the particulars of the products handled, and on the WWW page organization.

[0067] It should be noted that, as described above, the required detection of unauthorized use in an electronic commerce transaction system must be performed in real time and, furthermore, this detection is usually performed using a plurality of data items, so the analysis of such data imposes a load on the server processing.

[0068] As a countermeasure in this respect, for example an order of priority of use in arriving at the actual decision is given to the various items of data of the individual model and general model, and it is arranged that these items of data are utilized for detection of unauthorized use by using the data that are higher in order of priority first. In this way, it is possible to reduce the load on the server by arranging that detection of an unauthorized client can be achieved by verification with as few data items as possible.

[0069] Also, it is arranged that, even in the condition that a decision regarding whether or not access constitutes unauthorized use has still to be reached, all of the data representing the access condition of the client is uniformly saved and accumulated as the access history information of the client, irrespective of whether or not such access does

in fact constitute unauthorized use. It may then be arranged, if necessary, for the conditions of client access to be reflected in the criteria and state transition rules for identifying unauthorized use when performing statistical processing.

[0070]

[Embodiments] Finally, as an embodiment, application of an example of the device described above and an example of the method to an actual electronic commerce transaction system will be described.

[0071] (First embodiment)

. Example of an electronic commerce transaction system for performing sale of articles

In this example, a product catalogue is presented on a WWW server on the Internet, and a client can perform selection and purchase of these products, and, if necessary, settlement of accounts. In this case, since no financial damage can occur simply as a result of perusal of the products, unauthorized use need only be detected prior to performance of settlement.

[0072] Consequently, detection of an unauthorized client can be performed using the large quantity of data collected immediately prior to performance of settlement from the time point of commencement of access of the server by the client: errors in detection of unauthorized clients can thereby be reduced. It should be noted that such errors in detection may include both misidentification of access by a regular client as access by an unauthorized client or misidentification of access by an unauthorized client as access by a regular client.

[0073] (Second embodiment)

. Example of an electronic commerce transaction system that provides information to members

This example consists in an electronic commerce transaction system that provides information exclusively to clients who have registered beforehand. The difference between this example and the example of the previous electronic commerce transaction system for

performing sale of articles lies in that it is not sufficient merely to detect unauthorized use before settlement: rather, it is necessary to detect unauthorized use, and to exclude this, as early as possible from the time point at which perusal of the information by the client commences.

[0074] Reasons for this that may be mentioned include that, in the case of an electronic commerce transaction system of this type, the information that is provided itself has value, so it is indispensable to detect at an early stage unauthorized use, in order to minimize the damage due to leakage of information, and also that settlement is not performed every time information is accessed, so the period allowed for settlement is long.

[0075] It should be noted that although, in the case of this example, in contrast to the example of an electronic commerce transaction system in which sale of articles is performed, no exchange of funds based on sale of articles takes place, so it is necessary to identify an unauthorized client solely from the data regarding the actions of this client in the WWW server, there is no difference at all regarding the basic constitution of the device. It is merely that the decision data and criteria in respect of an unauthorized client are different.

[0076] Hereinabove, an Internet system using the WWW was described by way of example of a client/server system with reference to a mode of implementation of the present invention and first and second embodiments thereof. However, the present invention can of course be applied to any desired type of clients/server system or user/provider systems capable of executing electronic commerce transactions. Also, the present invention is not necessarily restricted solely to the means and techniques described above and can be implemented with suitable modifications within a range in which the objects of the present invention are achieved and the following beneficial effect obtained.

[0077]

[Beneficial effect of the invention] As described above, according to the present invention, a plurality of data items of various types issued after commencement of access of the server by the client are acquired, this acquired plurality of data items are respectively compared with a plurality of data items subsequently obtained after new access, every time such new access is executed, and a decision as to whether or not this new access represents unauthorized use is made in accordance with the result of this comparison.

[0078] It thereby becomes possible to detect unauthorized use of the system by an unauthorized user or unauthorized client, based on the results of monitoring the ordinary actions of regular users or regular clients, and also becomes possible to obtain a grasp of the series of actions performed by the same user or same client and, furthermore, it becomes possible to detect unauthorized use of the system, based on the mode of action of typical users or clients. As a result, the possibility of financial damage to users of an electronic commerce transaction system whereby for example sale of articles is performed becomes extremely low.

[Brief description of the drawings]

[Figure 1] This is a block diagram showing the constitution of a device for detection of unauthorized use according to a mode of implementation of the present invention.

[Explanation of the reference symbols]

α: device for detecting unauthorized use of electronic commerce transaction system

1...access data extraction means

2...data accumulation means

3...access data

4...individual models

5...general model

6...decision criterion supplying means

7...unauthorized use decision means

[Figure 1]

α: device for detecting unauthorized use of electronic commerce transaction system